Remarks

Claims 1-72 are pending in the application. Claims 1-72 are rejected. Claims 2-3 and 12-72 are cancelled. Claims 1 and 4-11 are amended. No new matter is added. All rejections are respectfully traversed.

The invention re-authenticates and protects wireless communication security. Using a key lease generated by performance of a primary authentication protocol, a secondary authentication protocol is performed between a wireless client electronic system (client) and a wireless network access point electronic system (AP). The key lease includes a key lease period for indicating a length of time in which the key lease is valid for using the secondary authentication protocol instead of the primary authentication protocol. If the secondary authentication protocol is successful, a session encryption key is generated for encrypting communication traffic between said client and said AP.

A hash function and encryption key from the key lease are applied to at least first and second random numbers to generate at least one session encryption key for use upon the successful completion of the secondary protocol. The invention is a useful solution to ensure the AP accepts replayed data frames upon subsequent performances of the secondary authentication protocol by wireless clients.

Support for elements a) and b) of claim 1 can be found in the parent (now granted U.S. Patent 6,920,559) of the present CIP application as well as between page 1, line 1 and page 36, line 7 of the present application. Support

for claim elements a(i) – a(iii), b(i) of Independent claim 1, and all of the remaining dependent claims can be found only between line 9 of page 36 and line 14 of page 41 of the present application.

Claims 1, 12, 23, 34-36, 47-49, and 60-62 are rejected under 35 U.S.C. 102(b) as being anticipated by Wood, et al., (U.S. 6,609,198 – "Wood"). Claim 1 is pending.

Wood describes a security architecture that provides a single sign-on for multiple information resources. Each information resource is assigned a trust level, and each trust level requires a different authentication scheme. Wood authenticates to information resources using different authentication schemes depending on the resource. In contrast, the invention uses primary and secondary authentication protocols to authenticate to a wireless AP. Therefore, the invention generates a session encryption key only after the performance of two inter-dependent authentication protocols. Wood generates a session encryption key for a particular information resource after the single performance of an authentication scheme required by a trust level associated with the resource. Further still, Wood is not directed to authenticating a wireless client device to a wireless AP, as claimed. Wood can never be used to anticipate what is claimed.

Claims 2-6, 13-17, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood in view of Dole (U.S. 6,628,786). Claims 4-6 are pending.

As stated above with respect to claims 1, 12, 23, 34-36, 47-49, and 60-62, Wood never describes wireless client device authentication to an AP at all. Dole fails to cure the defects of Rune. Dole describes a random number generation method used for encrypting communications between computers.

The Examiner's assertion that Dole teaches generating a first random number associated with said client and a second random number associated with said AP as claimed, is pure conjecture because there is never any description of associating random numbers with a computer such as a client or AP in col. 6, lines 5-27, see below:

Referring now to FIG. **3**, a flowchart illustrating a method of implementing the present invention is presented. Normally, the method of the present invention will be implemented as a computer program ("application") residing on a host computer. However, it will be appreciated by those skilled in the art that the method of the present invention may be implemented through the use of electronic hardware or through the use of a combination of hardware and software.

The random number generator is started with a request for random numbers (step **50**). Normally, the internal state of the random number generator will have previously been set, based upon a prior operation. Next, the application will check to determine whether any additional sources of entropy have been received (step **52**). Additional sources of entropy may consist of prior secret session keys, nonces, private/public key pairs generated for encryption protocols such as RSA or random key values utilized to implement the Diffie-Hellman key exchange protocol. If no additional sources of entropy have been received, the application will proceed to generate random numbers based on the existing internal state (step **60**).

The Examiner is requested to specifically point out exactly which words above mean generating a first random number associated with said client and a second random number associated with said AP, as claimed. The applicants see only random number generation for encryption purposes. Further still, there is no teaching of primary or secondary authentication protocol, or re-authenticating.

The hashing described in Dole is for encryption of a particular message and has nothing to do with a secondary authentication protocol using a key lease from performance of a primary authentication protocol, as claimed.

Claims 7-11, 18-22, and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood in view of Dole and in further view of Kessler, et al., (U.S. 6,789,147 – Kessler). Claims 7-11 are pending.

Claimed is using said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a second media access control (MAC) address associated with said AP, and a hash function to determine said first and second session encryption keys. The section at col. 5, lines 18-37 referenced by the Examiner does not even hint at generating first and second session encryption keys based on the explicitly recited elements above, see, e.g., col. 5, lines 29-32, below:

conjunction with FIGS. **3–8**. Additionally, such security operations could include, but are not limited to, a request to (1) generate a random number, (2) generate a prime number, (3) perform modular exponentiation, (4) perform a hash operation, (5) generate keys for encryption/decryption, (6) perform a hash-message authentication code (H-MAC) operation, (7) perform a handshake hash operation and (8) perform a finish/verify operation. 30 35

There is nothing above that describes the explicitly claimed combination of elements to generate the first and second session keys, as claimed.

The same is true for the claimed applying a HMAC-MDS algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key. There is no description of applying HMAC-MDS algorithm to the particular concatenation to produce either a first or second session key as recited in the claims. The Examiner is also reminded that the invention re-authenticates using a second authentication protocol and a key lease from a primary
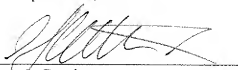
10

authentication protocol. No such thing is ever considered by Rune, Dole, or Kessler.

It is believed that this application is now in condition for allowance. A notice to this effect is respectfully requested. Should further questions arise concerning this application, the Examiner is invited to call Applicant's attorney at the number listed below.

Please charge any shortage in fees due in connection with the filing of this paper to Deposit Account 50-3650.

Respectfully submitted,
3Com Corporation,

By

350 Campus Drive
Marlborough, MA 01752
Telephone: (508) 323-1330
Customer No. 56436

Andrew J. Curtin
Attorney for the Assignee
Reg. No. 48,485